PERIPHERAL DEVICE FOR A COMPUTER SYSTEM

Related Application Data

This application claims priority from provisional application 60/158,015, filed October 6, 1999.

Brief Description of the Drawing

Ins A1

The present disclosure memorializes certain improvements to the subject matter detailed in pending application 09/343,104 (June 29, 1999), and 09/292,569 (April 15, 1999), the disclosures of which are incorporated by reference.

The cited '104 application details a variety of systems in which objects interact with computer devices. The objects can be physical objects, marked with machine-readable indicia, such as digital watermarks. Optical input devices, such as webcams, are used to capture image data from the object, so that the computer device can recognize the object and respond accordingly.

In the '104 application, the disclosed technology was referred to by the name "Bedoop." The present assignee now markets such technology under the Digimarc MediaBridge name. The former term is used in this disclosure.

One form of optical input device usable in such systems is a mouse-like peripheral that includes an optical sensing system. The optical sensing system can comprise a 1D array of plural optical sensors (e.g., CCD, CMOS, etc.), or a 2D array. Such devices are already known in other contexts, e.g., the Microsoft IntelliMouse with IntelliEye technology. That device includes a multi-element CMOS optical sensor integrated on an IC with various detector and processing circuitry, operating in conjunction with a short focal length imaging lens and an LED illumination source. The circuitry tracks movement of patterns across the sensor's field of view, by which the mouse's movement can be

deduced. The Microsoft product collects 1500 data sets per second – a frame rate much higher than is needed in most embodiments of the assignee's Bedoop technology.

Such a mouse-like peripheral can omit the buttons and position-sensing features commonly provided on traditional mice, yielding a simple desk-facing palm camera that generates frames of data corresponding to a small area under the sensor portion of the mouse. More typically, however, the peripheral includes the buttons, roller wheels, and/or X-/Y- position sensing arrangements of traditional mice so that button and positional forms of data input can be exploited in interacting with the Bedoop application.

The optical data collected by the sensor can be processed within the peripheral's processor to extract the steganographically encoded binary Bedoop data therefrom. Or this processing burden can be undertaken by the associated computer system, with the peripheral simply processing and formatting the raw sensor data into sequential frames of image data to be output to that system.

Any form of hand-held scanner - whether of the type just described or others known in the art - offers a convenient way to interact with catalog advertising. Imagine a traditional paper catalog, e.g., from L.L. Bean, Inc., or Lands End. Each image in the catalog is Bedoop-encoded with a code that identifies the depicted product. A user browsing through the catalog, on seeing a product of interest, places the scanner over the picture (and optionally may be required to push a button or otherwise signal to initiate further processing). The scanner detects the Bedoop data and relays it to an associated computer (optionally with data identifying the consumer). The computer polls a remote server computer maintained by the merchant, which responds with data corresponding to the item depicted in the scanned image. This returned data can include data indicating the sizes available, data indicating the colors available, data indicating the variant styles available, flag bits indicating whether each item is in stock, etc. This returned data can be presented to the consumer – typically on a display device but alternatively in audible form.

Preferably, the customer's body measurements (waist size, inseam length, neck size, etc.) are stored in a user profile, either on the local computer or at the merchant's server computer. This allows the system to customize the data presented to the user – e.g., showing the color options and availability only for the depicted shirt in a 16 inch neck and a 34 inch sleeve length.

If necessary, the user can select among the color or style options, using the handheld input device (either buttons, gestures, etc.), or any other input device. Or the item may be one for which no further specifications are needed. In either event, once the desired product has been sufficiently specified, the user can signal the system to place the order. Payment and shipping details can be arranged through any of the great variety of techniques known in the art, e.g., by charging to a credit card number and shipping to an address on-file with the merchant.

While scanning peripherals of the type described above are typically wired to an associated host system, wireless links (e.g., radio, infrared, ultrasonic, etc.) can of course be used, freeing the user from the constraint imposed by the cable.

Another use of the technology detailed in the '104 application (and other applications and patents of the present assignee, including patent 5,841,886 – incorporated herein by reference) is to control building access (or facility access, or room access, etc.) through a combination of an ID card, Bedoop technology, and proximity detection technology.

The ID card can be a badge or the like having a steganographically-encoded photograph of the bearer. The card further includes a proximity ID device, such as an unpowered electronic circuit that is excited and detected by a radiant field from an associated proximity detector, providing a unique signature signal identifying a particular individual.

The building can be provided with an image sensor (such as a video camera or the like), an associated Bedoop detection system, and the proximity detector. When a user wearing the badge approaches, the proximity detector signals the camera to capture image data. The Bedoop detection system identifies the badge photograph (e.g., by clues as are described in the prior applications, or without such aids),captures optical data, and decodes same to extract the steganographically-embedded data hidden therein. The access control system then checks whether the badge ID discerned from the proximity sensor properly corresponds to the Bedoop data extracted from the photograph on the badge. If so, access is granted; if not, the data is logged and an alarm is sounded.

By such arrangement, premises security is increased. No longer can proximity-based access badges be altered to substitute the picture of a different individual. If the photo is swapped, the proximity system ID and the embedded photo data will not match, flagging an unauthorized attempted access.

The same principles are applicable in many other contexts – not limited to RF-based proximity detection systems. For example, the data decoded from the photograph can be compared against other forms of machine-sensed personal identification associated with the badge. These include, but are not limited to, bar code IDs, mag-stripe ID cards, smart cards, etc. Or the comparison can be with an identification metric not associated with the badge (e.g., retinal scan, voice print, or other biometric data).

Having described an illustrated the principles of our inventions with reference to specific embodiments, it will be recognized that the principles thereof can be implemented in many other, different, forms. Moreover, the particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substituting of these teachings with teachings in the incorporated-by-reference applications and patent are also contemplated.